Осторожно, мошенники!

Борьба с киберпреступностью является одной из сложных задач не только в городе-курорте, но и в целом во всех регионах страны.

Преступные схемы стремительно развиваются и совершенствуются. В 2021 году преступления с применением IT-технологий составили четвертую часть от всех зарегистрированных преступлений в Сочи.

Несмотря на информированность граждан о типичных случаях мошенничества, которые совершаются с использованием мобильной связи, уровень киберпреступлений в настоящее время довольно высок. Злоумышленники совершенствуют способы мошенничества, о которых потенциальные жертвы не знают.

Так распространение получила мошенническая схема с незаконным использованием подменных абонентских номеров (используются номера банков, в том числе Центрального Банка России, подразделений МВД России, Следственного комитета России, органов прокуратуры Российской Федерации).

При этом для реализации подмены номера звонящего используются не только технологически сложные системы, но и более доступные варианты, например, Telegram-бот, который позволяет организовывать звонки с подменой номера прямо из мессенджера.

Также злоумышленники в целях реализации мошеннических схем и оказания психологического воздействия на потерпевших используют и рассылают в мессенджеры поддельные повестки о необходимости явиться для допроса в качестве свидетеля, с использованием бланков правоохранительных и надзорных органов.

Типичными схемами мошенников, при которых последние получили доступ к денежным средствам граждан, явились такие случаи как:

1) получение потерпевшими SMS-сообщения или поступление звонков от якобы работников банка о том, что банковская карта заблокирована, а также произошла попытка списания денежных средств. «Сотрудник банка» просит граждан сообщить номер карты и PIN-код для ее перерегистрации. После сообщения потерпевшими запрашиваемых данных с их счетов списывались денежные средства;

2) на мобильный телефон потерпевших поступают SMS-сообщения о получении выигрыша, для получения которого необходимо отправить подтверждающее SMS-сообщение либо внести регистрационный «взнос» через систему электронных платежей. Однако после внесения на счет неизвестных лиц такого «взноса» никакого выигрыша потерпевшие не получают;

3) имеют место случаи, при которых через сайт магазина в сети «Интернет» граждане заказывают понравившийся им товар, однако после его оплаты потерпевшие ни только не получают заказ, но и лишаются уплаченных за него денег.

Анализ преступлений, связанных с мошенничеством с использованием информационно - телекоммуникационных технологий, показывает, что почти во всех случаях потерпевшие, потеряв бдительность, своими действиями упрощали преступникам доступ к своим денежным средствам.

В целях избежания подобных ситуаций напоминаем о необходимости быть внимательными и бдительными при совершении различных сделок с помощью Интернет-ресурсов, не выполнять никаких операций со своими банковскими картами по инструкциям неизвестных лиц по телефону!